Bird & Bird & Privacy & GDPR

Benoit Van Asbroeck, Partner
benoit.van.asbroeck@twobirds.com

Some key elements of the GDPR

General Overview	• New European legislation ("GDPR") directly applicable as from 25 May 2018 • Broad territorial scope • Strengthening of the obligations concerning the processing of personal data
Scope of application & Sanctions	• All GDPR obligations will apply to your organisation • Significant strengthening of sanctions
Clarification & strengthening of core privacy principles	• Strengthening of core privacy principles • Strengthened consent requirements • Your organisation will have to be able to demonstrate its compliance with the GDPR
Risk analysis & Accountability principle	Your organisation will have to: • assess risks for the rights and freedoms of individuals • implement measures that enable demonstrating that it anticipated its compliance with the GDPR • keep updated internal records of all personal data processing activities • perform Privacy Impact Assessments in certain cases • appoint an independent Data Protection Officer (subject to more in depth analysis) • identify all sub-contractors and situations where it acts as sub-contractor and review the contractual relationships
Reinforcement of individuals' rights	• Development of existing rights and creation of new rights for individuals • Strengthening of information requirements • Your organisation will need to be able to respond to individuals' requests for access to their personal data • Your organisation will have to erase processed data in certain circumstances • Your organisation will have to implement measures to respond to individuals exercising their rights
Security obligations & Breach notifications	• Your organisation will have to implement technical and organisational measures to ensure the security of personal data • Your organisation will have to notify data breaches within short deadlines, notably to the supervisory authority
How to get ready for the GDPR?	• The compliance programme requires deploying adequate resources • It is recommended to initiate the compliance process as soon as possible in order to be sufficiently ready by 25 May 2018 and avoid sanctions • A compliance programme usually takes place in several phases: 1. Awareness 2. Inventory and assessment of personal data processing 3. Identification of remedial actions 4. Prioritisation of remedial actions and implementation of measures 1. Control of compliance

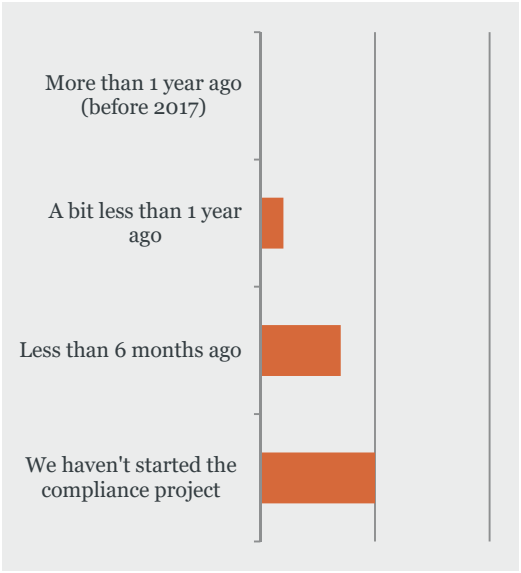
© Copyright Bird & Bird

Bird & Bird

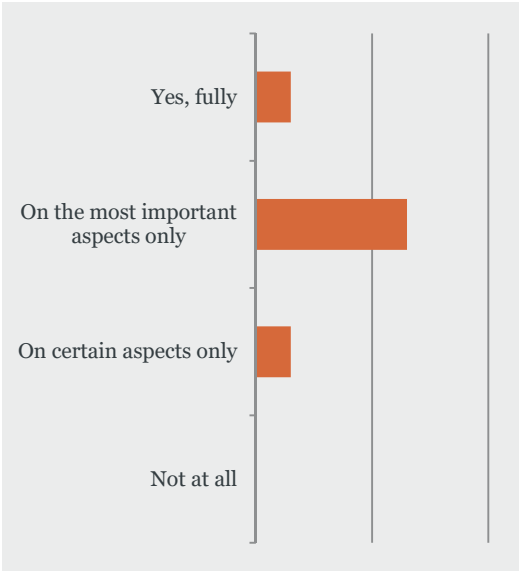
General questions

Survey

When did you start getting ready for the GDPR?



Do you believe your organisation will be ready by 25 May 2018?



© Copyright Bird & Bird

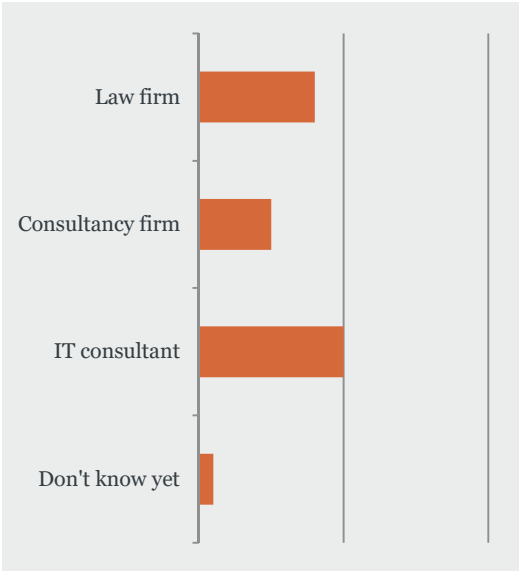
Bird & Bird

Externalising certain aspects?

Survey

According to you, the assistance of an external counsel is needed?

What type of external counsel do you rely on (if any)?



Externalising IT aspects (IT consultant)

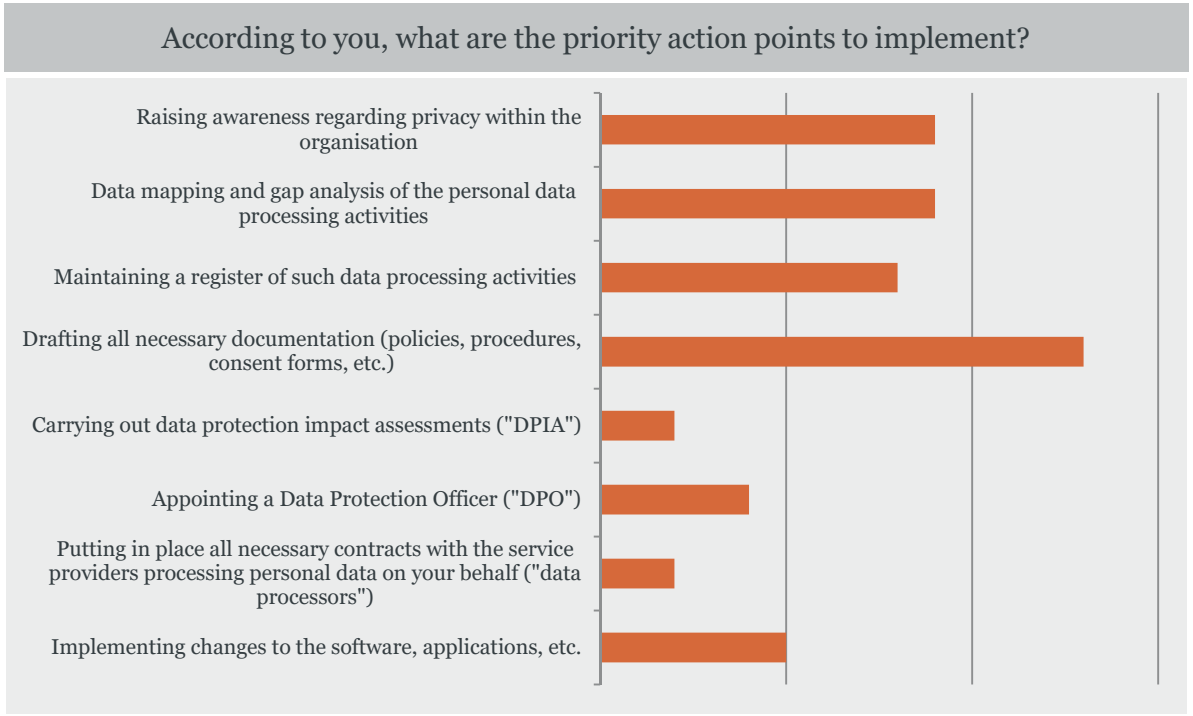
Two major IT-related tasks:

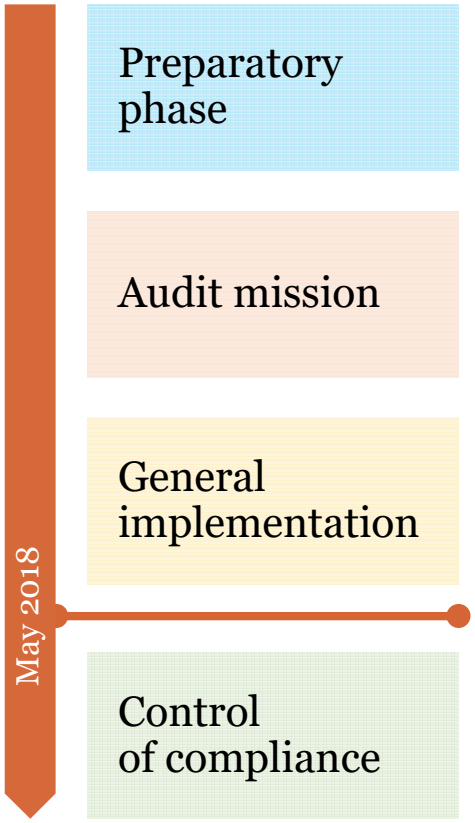
- Retrieve/map key IT aspects
  - the list of software and applications that involve the processing of personal data and the nature of such software/applications (off-the-shelf, tailor-made) including details about publishers, vendors, integrator, main functions of each software ...
  - the locations of the servers and the underlying service provider(s)
  - the internal policy with regard to updating/upgrading software
  - the list of cloud services and the storage of personal data on cloud services
  - the general security measures in place and the list of specific solutions used with respect to security
  - access restrictions and logs
  - the back-up/mirroring processes applicable within the organisation
  - the existence of (critical) 'shadow IT' practices within the organisation
  - etc.
- Retrieve/map IT-related agreements (i.e. licences + maintenance agreement + services agreements + SLAs)

© Copyright Bird & Bird

Setting priorities

Survey



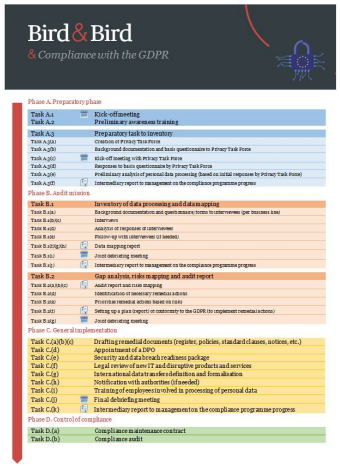


© Copyright Bird & Bird

Bird & Bird

Setting priorities

Methodology



Preparatory phase

- Kick-off meeting
- Preliminary awareness training
- Preparatory task to inventory

Audit mission

- Inventory of data processing and data mapping
  - Questionnaires, interviews, document analysis
- Gap analysis, risks mapping and audit report
  - Identification and prioritisation of remedial actions

General implementation

- Drafting remedial documents (register, policies, standard clauses, notices, etc.)
- Appointment of a DPO
- Security and data breach readiness package
- Legal review of new IT and disruptive products and services
- Data Protection Impact Assessment (where needed)
- International data transfers definition and formalisation
- Notification with authorities (if needed)
- Training of employees involved in processing of personal data

May 2018

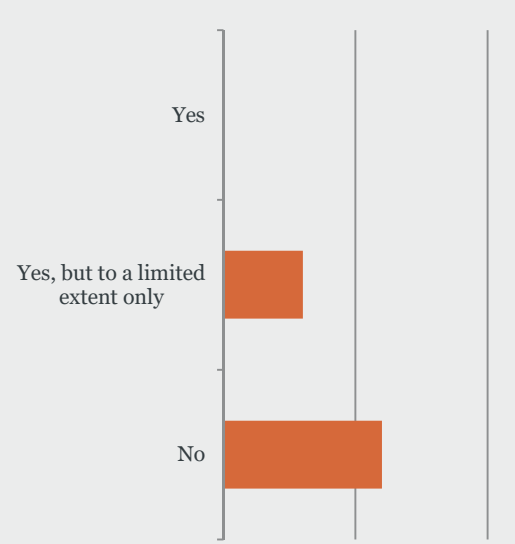
© Copyright Bird & Bird

Bird & Bird

Individuals' rights

Survey

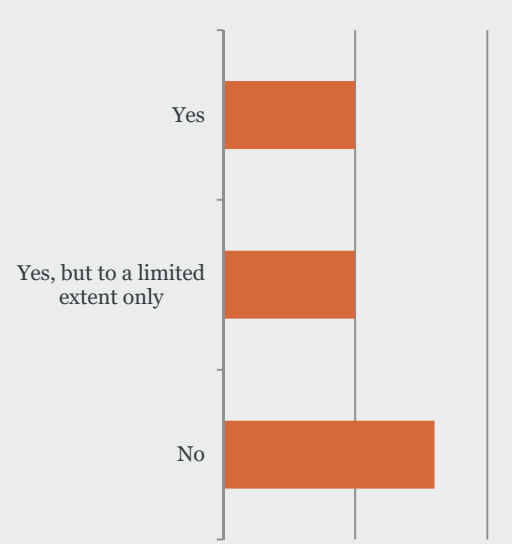
Do you expect many individuals to exercise their rights (access, erasure, portability, etc.)?



IT changes

Survey

Have you considered the implementation of changes to software, applications, etc.?



© Copyright Bird & Bird

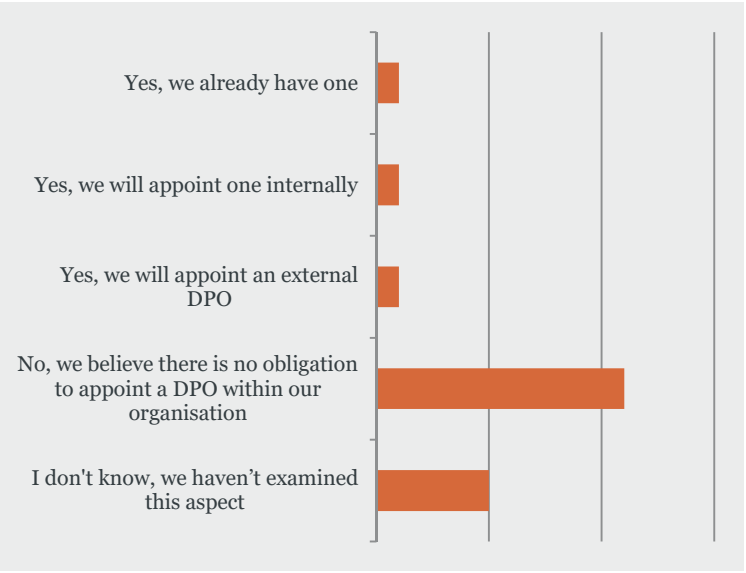
Bird & Bird

Data Protection Officer

Survey

Privacy

Do you believe (or know) that a DPO will need to be appointed?



Necessary to balance the pros and cons based on the company's particularities

Insourcing	Outsourcing
• Better understanding of the company and its internal workings • Easier access to the different departments processing personal data • Easier access to relevant information • Costs generally lower and better controlled (depending on the pricing arrangements) • Better understanding of the business sector and the company • Better knowledge of the internal IT resources and security measures • More pragmatic • Better placed to advise taking into account a risk-based approach • Better known within the company • etc.	• Easier to comply with the requirements of autonomy and independence • Higher likelihood of absence of conflict of interests • Costs of the continuing education included in the price arrangement • Easier replacement (temporary or definitive) in case of holidays, sickness, etc. (if outsourced to a legal entity) • Termination of the contract provided contractually • Liability agreed contractually • Easier to report objectively to the highest level of the management • Easier to accommodate special protection of the DPO provided in the GDPR • More resources available • etc.

Necessary to examine the different options and weigh their pros and cons

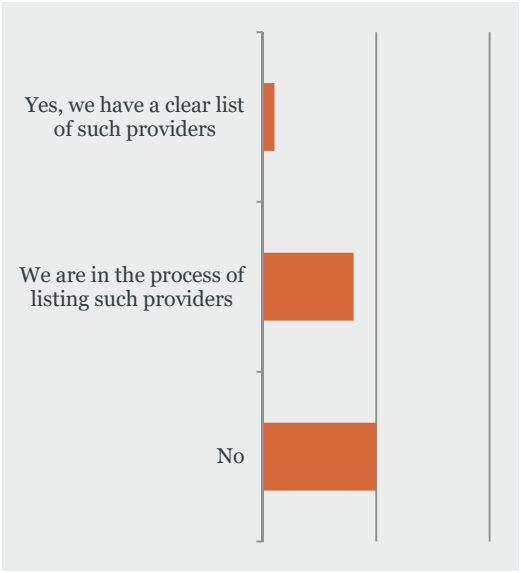
	Insourcing (employee of controller/processor)				Outsourcing	
	Internal promotion		New hire			
	DPO only	DPO + others tasks	DPO only	DPO + others tasks	Individual	Organisation (legal person)
OPTIONS	**1**	**2**	**3**	**4**	**5**	**6**
Autonomy and independence	8,3	6,7	9,7	7,3	10,0	10,0
Protection of the DPO	7,0	5,0	7,5	5,5	9,5	10,0
Conflict of interests	8,5	4,5	9,0	5,0	9,5	9,0
Expertise and professional qualities – General	8,3	7,3	9,0	8,0	8,7	10,0
Expertise and professional qualities – Specific	9,0	10,0	7,8	8,8	6,3	5,8
Tasks of the DPO	8,9	8,1	8,5	7,7	6,8	6,6
Fulfilling tasks	8,9	6,9	9,3	7,4	7,7	7,7
Obligations of the controller/processor	8,5	7,8	8,8	8,0	8,5	9,8

© Copyright Bird & Bird

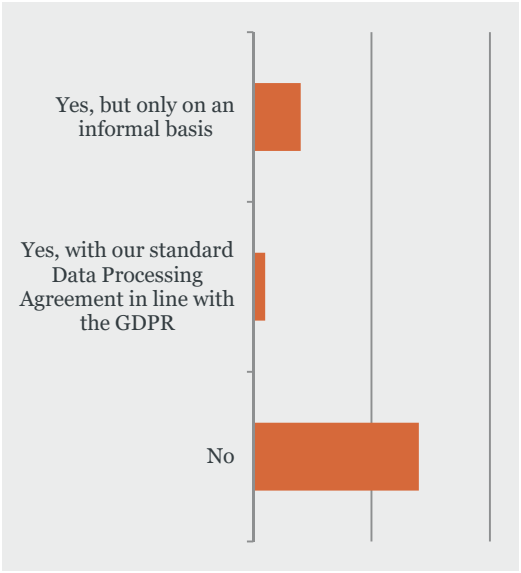
Service providers

Survey

Have you examined which service providers process personal data on your behalf?



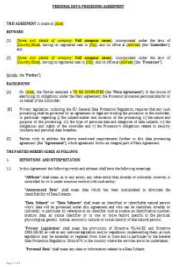
Have you contacted your service providers processing personal data on your behalf?



Relationship between "controllers" and "processors"

- Minimum contractual content imposed in the GDPR

- Despite minimum requirements, use of terms can make contract more favourable to data controller or data processor:
  - Tailor-made agreement taking into account variety of services
  - Specify general obligations: divide tasks and responsibilities
  - Define concepts (e.g. "without undue delay")
  - Specify tasks and obligations for data processor



- Practice of accompanying letters
  - Data processing agreement from data controller accompanied by letter whereby DPA is imposed on data processor

© Copyright Bird & Bird

Bird & Bird

Thank you & Bird & Bird

Benoit Van Asbroeck, Partner
benoit.van.asbroeck@twobirds.com

twobirds.com

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 12 New Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.